Extending and Securing Mail Services Using Mac OS X

Session 646

These are confidential sessions—please refrain from filming or taking pictures.

Enterprise IT

Extending and Securing Mail Services Using Mac OS X

Paul Schreiber
Screen Real Estate Agent
schreiber@apple.com

http://developer.apple.com/wwdc2005/

Introduction

- Securing
- Extending
- Account bundles
- Mac OS X Server GUI

What You'll Learn

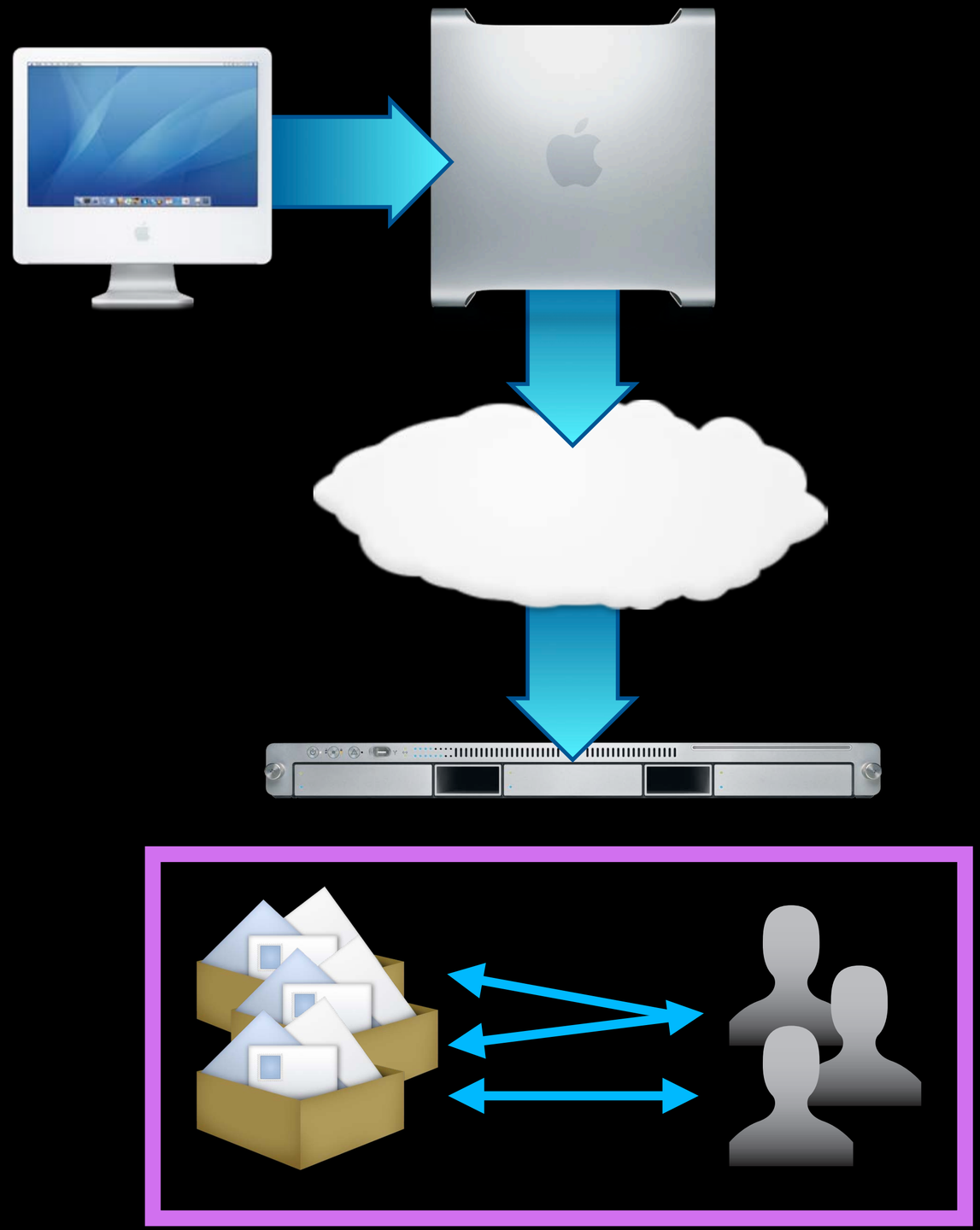
- Securing
  - Transport
  - Content
- Extending
  - Spam and viruses
  - Multiple domains
- Account bundles
- Mac OS X
  - Open source, open standards

Technology Framework

- Mail: IMAP, POP, SMTP
- Encryption: SSL, S/MIME, HTTPS, MD5, Kerberos
- Unix: Postfix, Cyrus, SpamAssassin, ClamAV, SquirrelMail
- Open source, standards-based
- Mac OS X Server provides improved ease-of-use

Internet Email

- Multiple domain names
- DNS servers
  - Multiple MX records
- User accounts
- Mailboxes
  - Virtual domains
  - Aliases
  - Many-to-many relationship



Overview

- Securing Mail Transport
- Securing Message Content
- Managing Multiple Domains
- Stopping Spam and Viruses
- Using Account Bundles

Securing Mail Transport

http://developer.apple.com/wwdc2005/

Overview

Securing Mail Transport

Securing Message Content

Managing Multiple Domains

Stopping Spam and Viruses

Using Account Bundles

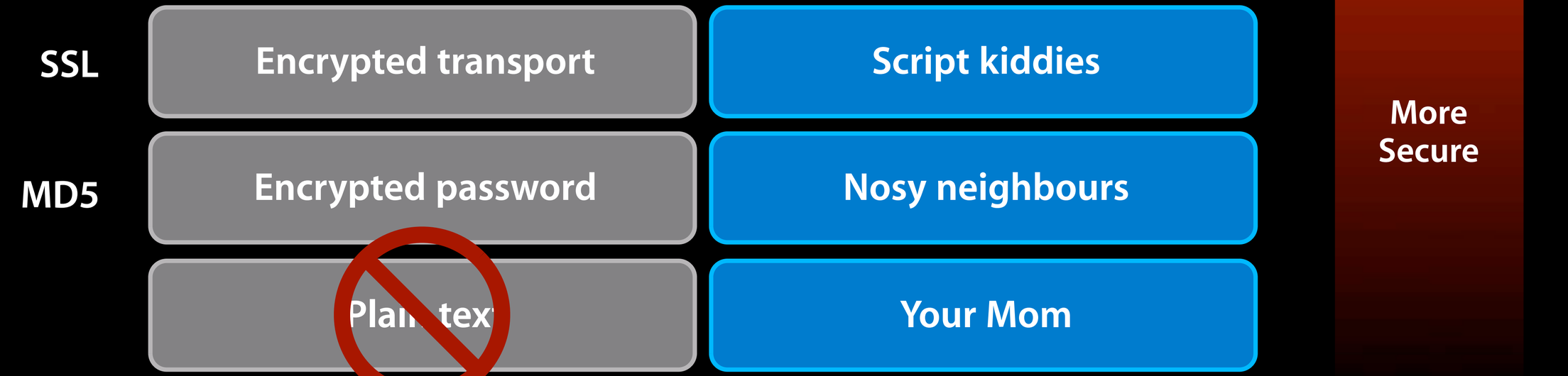
Security

- Security is a tradeoff
- Human factor is the weakest link
- Physical security
- Electronic security
  - Screen locking
  - Open firmware
  - Passwords
  - SSH
- Secure transport
- Secure content

Securing Transport: Motivation

- In the clear by default
- WiFi networks
  - Conferences, like WWDC
  - Coffee shops
  - Friends' houses

Authentication Methods



Security: SSL

- Cross-platform
  - Mac OS X, Windows, Linux, …
- Any client
  - Thunderbird, Eudora, Entourage, Outlook
- Very hard to break
- Gotchas
  - Weak passwords
  - In transit
  - Man-in-the-middle attacks

SSL: Certificates

- Must be trusted
- Purchase a certificate
  - Equifax, VeriSign, …
  - Cost: $30–$1790
- Create your own (self-signed)
  - Requires work on the client side
  - Cost: $0
- Become your own CA

Demo

Self-signed Certificates

Andrew Moon
moon@apple.com

SSL Demo

- Server
  - Create SSL certificate
  - Configure Mail server
- Client
  - Configure Mail client
  - Add root certificate to keychain

SSL on Panther Server

- Requires Terminal
- See “Creating Secure Transactions on Mac OS X Server Using SSL”

Instructions	developer.apple.com/server/security_ssl.html

Securing Message Content

http://developer.apple.com/wwdc2005/

Overview

Securing Mail Transport

Securing Message Content

Managing Multiple Domains

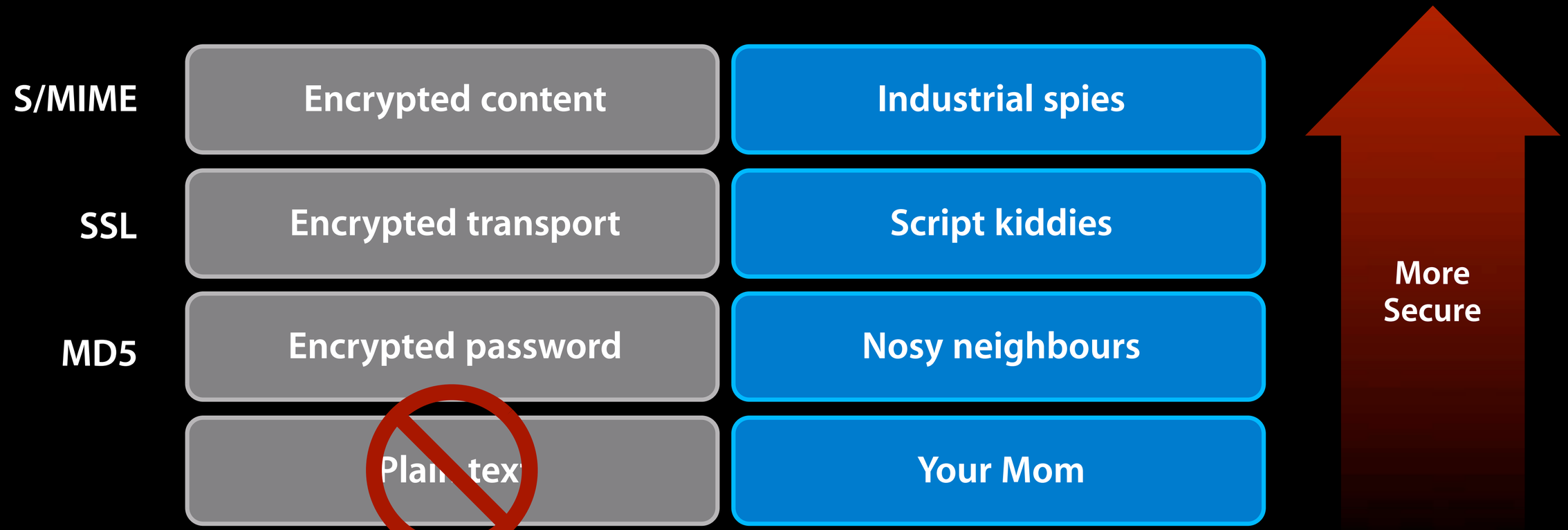
Stopping Spam and Viruses

Using Account Bundles

Signed and Encrypted Mail

- SSL is not always enough
- Message can still be read
  - In transit
  - On the client machine
  - On the server
- S/MIME lets you
  - Sign messages
  - Encrypt messages

Authentication Methods



S/MIME Benefits

- Signing
  - Ensures content was not modified
  - Makes no claim about who the sender is
- Encryption
  - Prevents messages from being read in transit and on disk

Using S/MIME

- Mail supports S/MIME
- Can sign right away
- Need public key to encrypt
  - Receive a signed message
  - Retrieve from server (e.g. LDAP)

Obtaining S/MIME Certificates

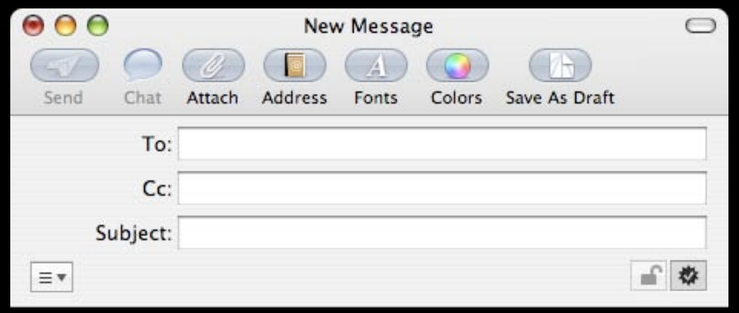
- Third-party vendors
  - Thawte
    - “Freemail member” by default
  - Verisign
- Be your own CA
- File types
  - .p7 (certificate)
  - .p12 (certificate and key)
  - .exe (Thawte .p7 files using Safari)
  - Requires 10.3.4 or better

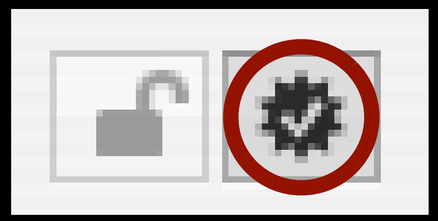
Deleting Certificates

- Don’t delete expired certificates from other people
- When deleting your certificate, remove private key

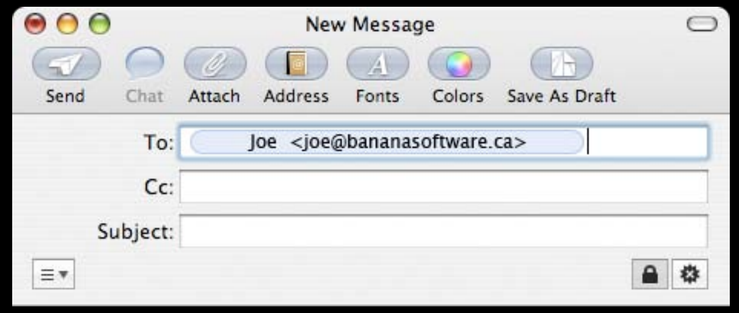
S/MIME in Action

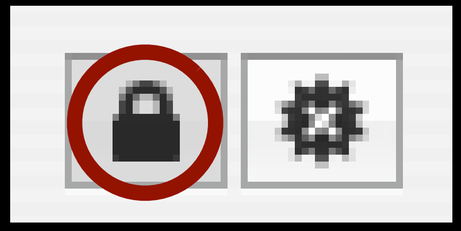
Signed



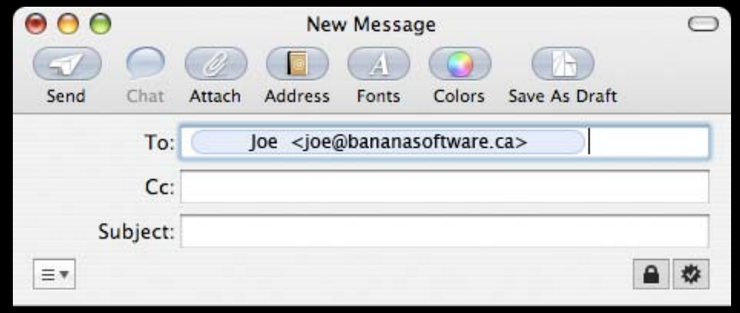


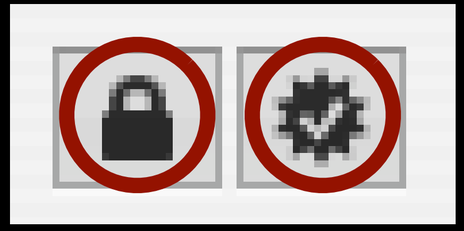
Encrypted





Signed and encrypted





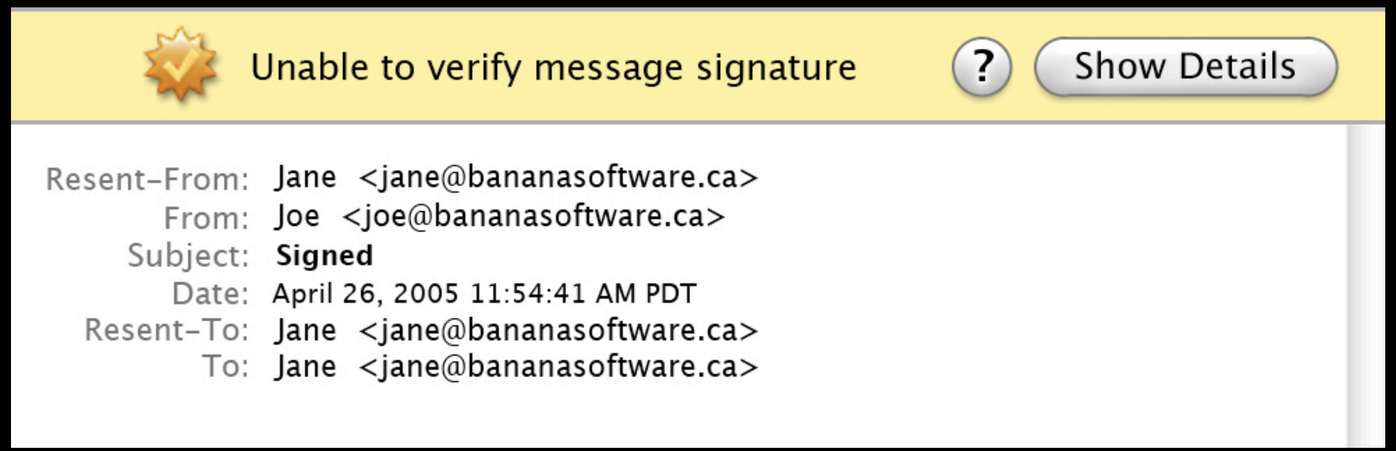
Receiving S/MIME Mail

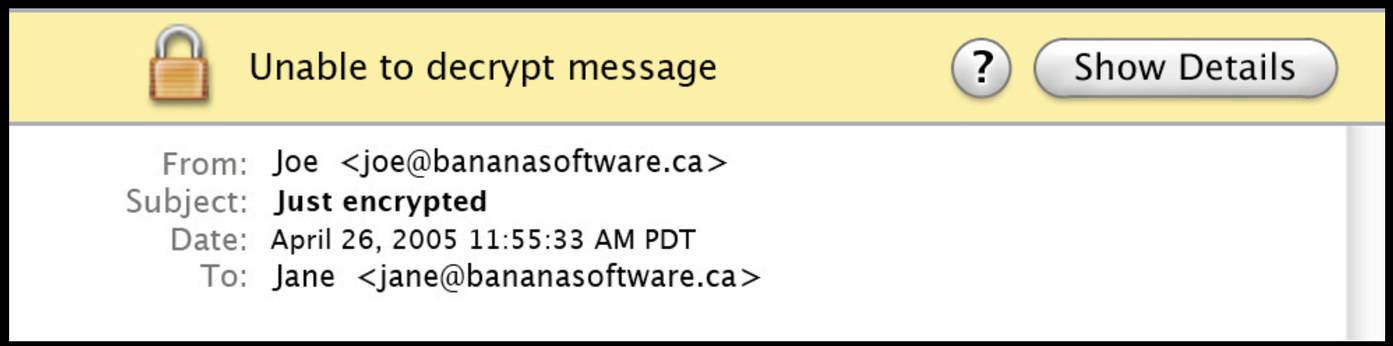
From: Joe <joe@bananasoftware.ca>
Subject: **Signed**
Date: April 26, 2005 11:54:41 AM PDT
To:
Security:

From: Joe <joe@bananasoftware.ca>
Subject: **Re: hello: signed**
Date: April 26, 2005 2:37:30 PM PDT
To:
Security:

From: Joe <joe@bananasoftware.ca>
Subject: **Signed and Encrypted**
Date: April 26, 2005 2:46:36 PM PDT
To: Jane <jane@bananasoftware.ca>
Security: Encrypted, Signed

S/MIME Problems





Managing Multiple Domains

http://developer.apple.com/wwdc2005/

Overview

Securing Mail Transport

Securing Message Content

Managing Multiple Domains

Stopping Spam and Viruses

Using Account Bundles

Managing Email Addresses

- One domain
- Virtual domains (shared namespace)
- Virtual hosting (separate namespace)
- Advanced virtual hosting

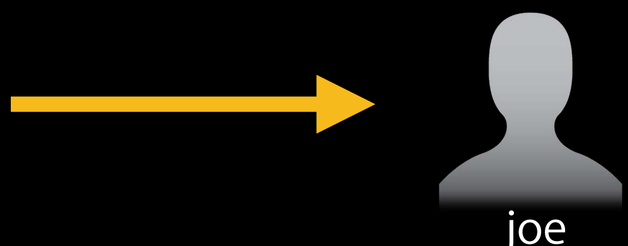
Configuration

- Two ways to do it
  - Mac OS X (Open Directory)
  - Postfix configuration files

One Domain

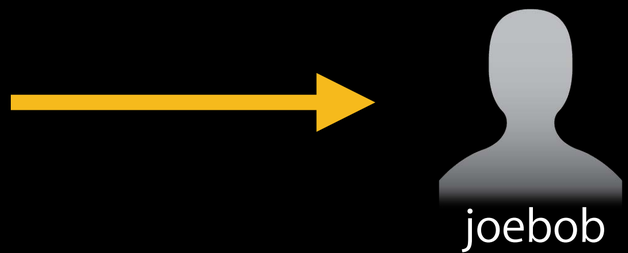
- No special configuration
- Create accounts

joe@bananasoftware.ca



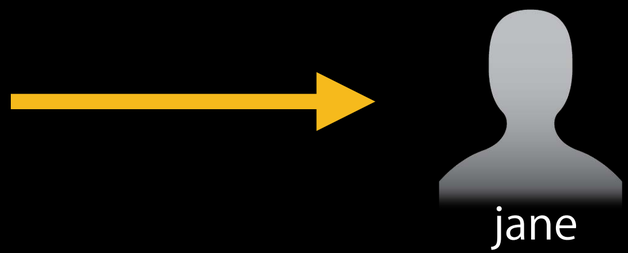
joe

joebob@bananasoftware.ca



joebob

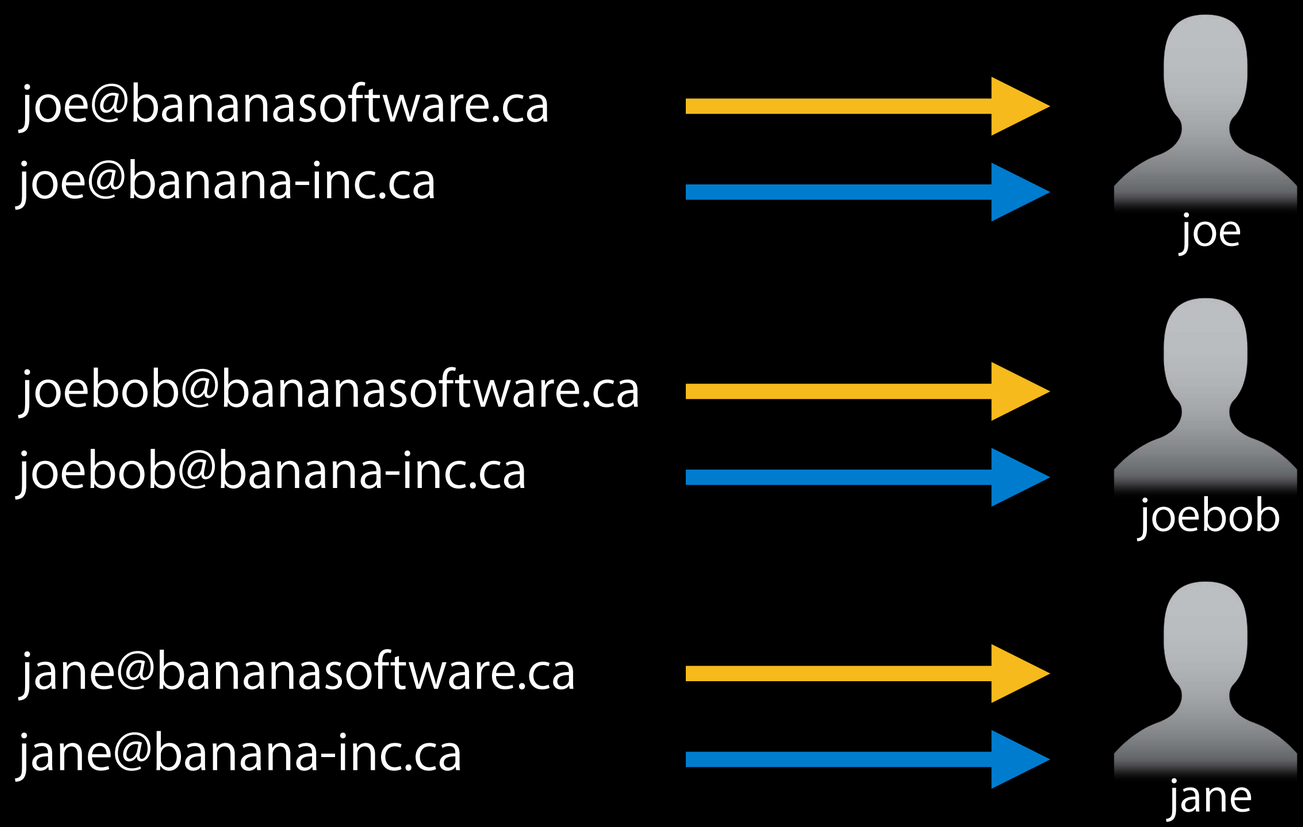
jane@bananasoftware.ca



jane

Virtual Domains

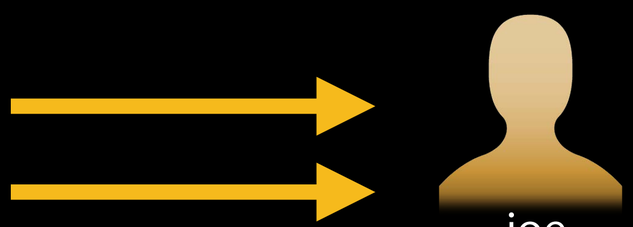
- Shared namespace
- Multiple domains
- Useful for aliasing domains
  - bananasoftware.ca
  - banana-inc.ca



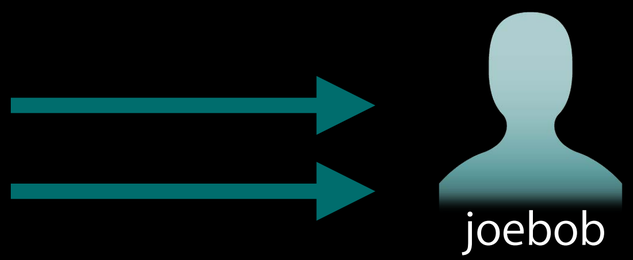
Virtual Hosting

- Multiple namespaces
- Multiple domains

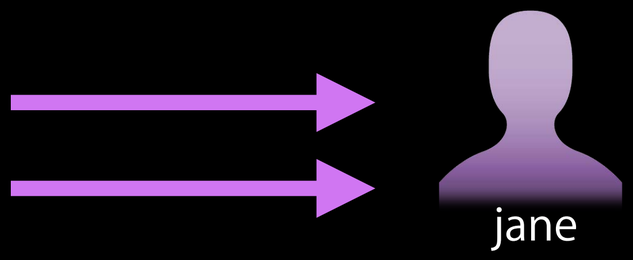
joe@bananasoftware.ca
info@bananasoftware.ca



joe@starfruit.ca
info@starfruit.ca



jane@guava.ca
info@guava.ca



Demo

Open Directory

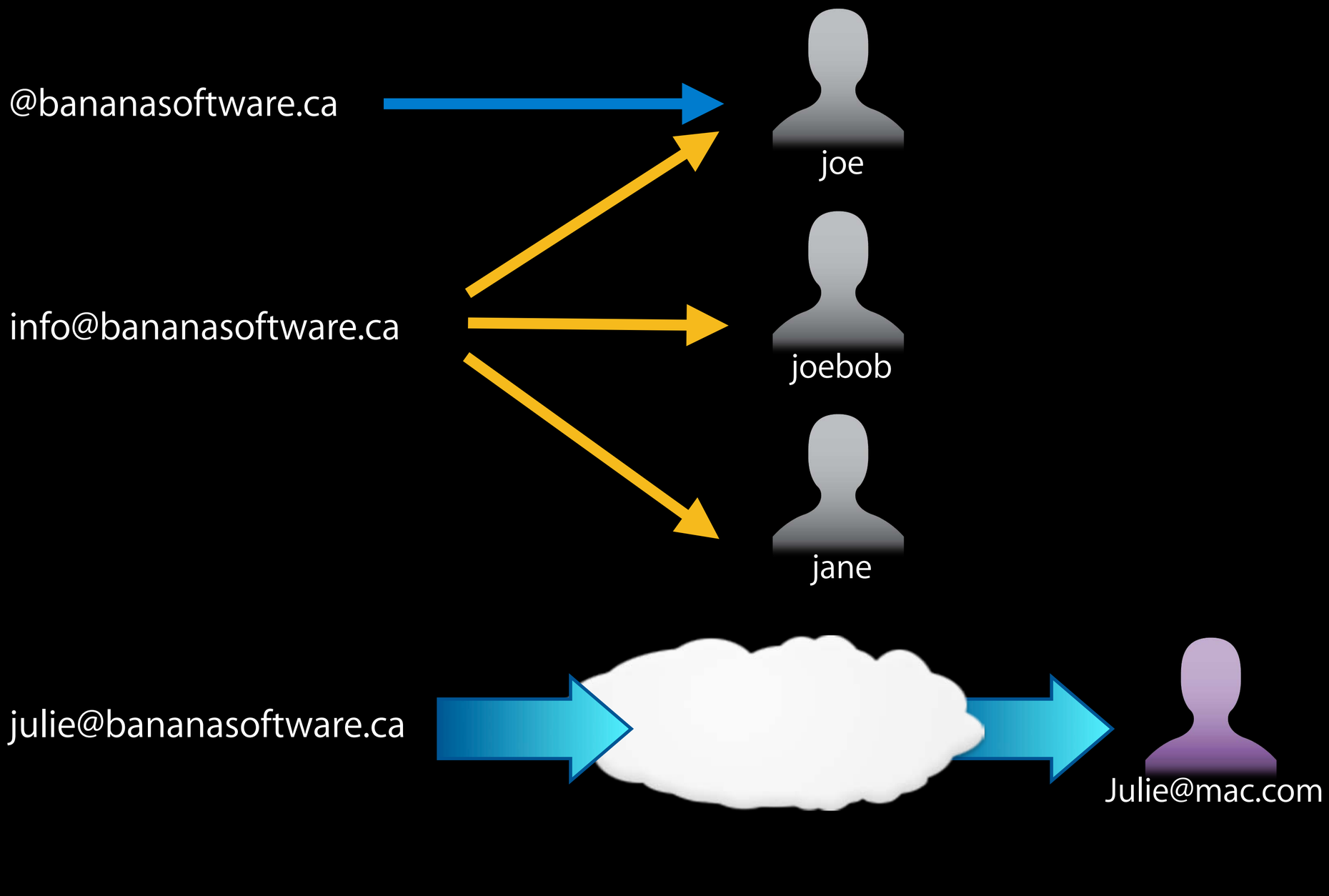
Andrew Moon
moon@apple.com

http://developer.apple.com/wwdc2005/

Open Directory

- Use Workgroup Manager
  - Use “short name” field
  - Keeps all configuration in one place

Advanced Virtual Hosting



Sendmail-Style Virtual Domains

- One server, two domains
- Users receive mail for the other domain, i.e. spam

	Joe	Jane
domain	bananasoftware.ca	guava.ca
joe@guava.ca	joe	—
joe@bananasoftware.ca	joe	—
jane@guava.ca	—	jane
jane@bananasoftware.ca	—	jane

Postfix-Style Virtual Domains

- One server, two domains
- Virtual hosting

	Joe	Jane
domain	bananasoftware.ca	guava.ca
joe@guava.ca	—	—
joe@bananasoftware.ca	joe	—
jane@guava.ca	—	jane
jane@bananasoftware.ca	—	—

Virtual Hosting Features

- Have one email address go to multiple people
  - Local and remote accounts
- Have an email address exist without a user account
- Provide a “catchall” address
- Mitigate dictionary attacks
  - If joe@bananasoftware.ca exists, and joe@guava.ca does not, mail to joe@guava.ca will bounce

Demo

Postfix Configuration Files

Andrew Moon
moon@apple.com

http://developer.apple.com/wwdc2005/

Configuration

- Postfix
  - Accessible by standard unix tools
  - Compatible with non-Mac servers running Postfix

Postfix Configuration File

- Edit `/etc/postfix/main.cf`
  - Add `virtual_alias_maps = hash:/etc/postfix/virtual`
- Edit `/etc/postfix/virtual`
  - Add needed aliases
  - `postmap /etc/postfix/virtual`
- Restart the server
  - `postfix reload`

Stopping Spam and Viruses

http://developer.apple.com/wwdc2005/

Overview

Securing Mail Transport

Securing Message Content

Managing Multiple Domains

Stopping Spam and Viruses

Using Account Bundles

Unwanted Email

- Spam
  - Blacklists (RBLs)
  - SpamAssassin
  - Challenge-response
  - Whitelists
- Viruses and worms
  - Mac users not typically harmed
  - Annoying, waste bandwidth
  - Be a good Internet citizen
  - You may have non-Mac clients
- Backup MX needs protection, too
  - Exploited by spammers

Realtime Blackhole Lists

- Upside: dramatic decrease in spam
- Downside: false positives
- Many lists
  - rbls.org—live query
  - rfc-ignorant.org
  - spamhaus.org
  - ordb.org
  - njabl.org
  - spamcop.net

SpamAssassin

- Highly configurable
- Per-user preferences
  - Whitelists
  - Custom scoring rules
- How it works
  - Rules
  - Bayesian filtering
  - RBLs
  - Messages meeting a threshold marked as spam
- Attractive target for sophisticated spammers

Viruses

- Tiger includes ClamAV
- Scan email for viruses
  - Delete
  - Bounce—bad idea
  - Quarantine
- Notification options

Demo

SpamAssassin
ClamAV

Andrew Moon
moon@apple.com

http://developer.apple.com/wwdc2005/

Using Account Bundles

http://developer.apple.com/wwdc2005/

Overview

Securing Mail Transport

Securing Message Content

Managing Multiple Domains

Stopping Spam and Viruses

Using Account Bundles

Account Bundles

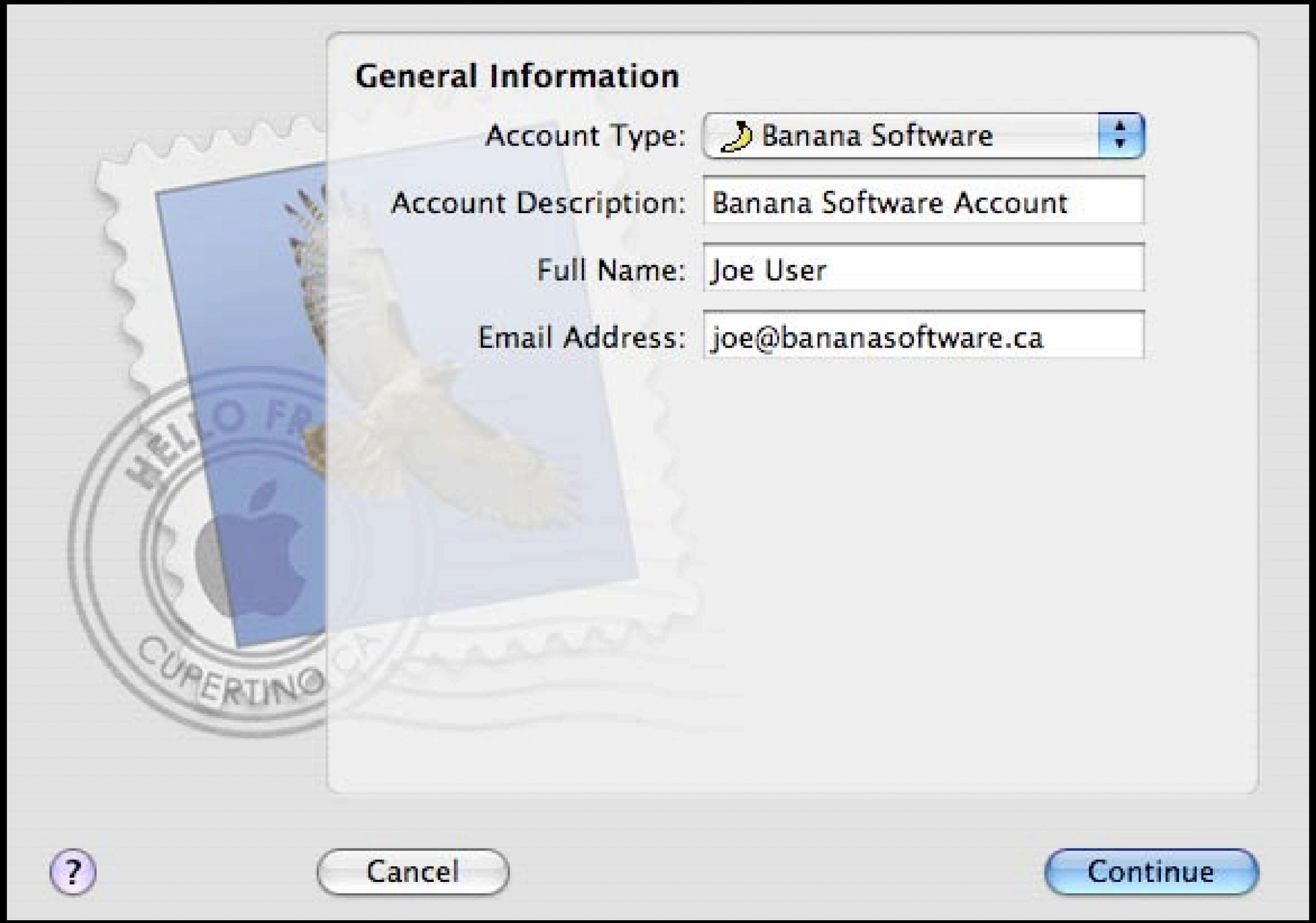
- Extend Mail’s setup assistant
- Make account configuration easy

Configuration Details

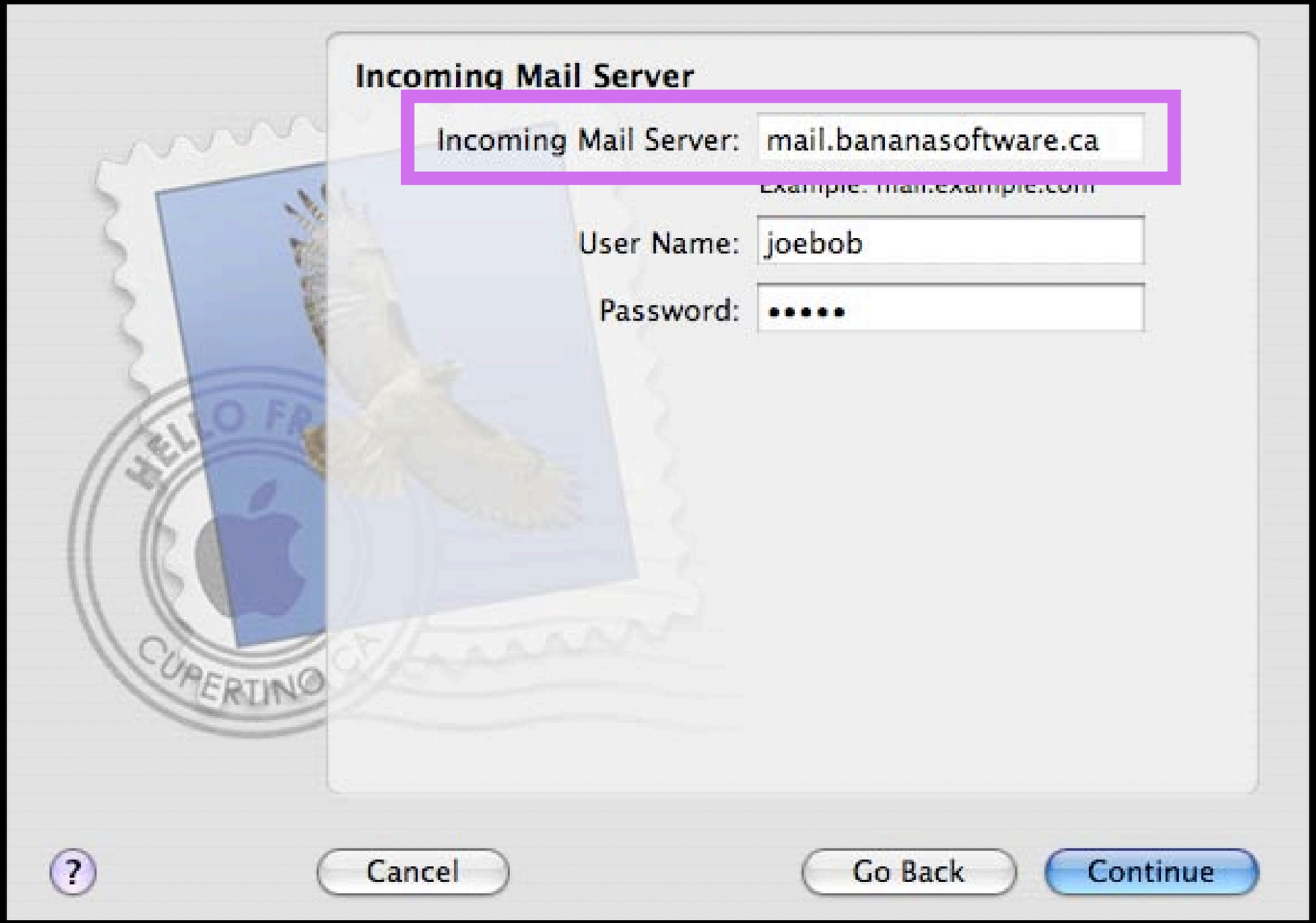
- Account name
- Server name
- Authentication type
- Email address domain name
- Email address = account name
- SSL state
- Support URL
- Localizable

Preconfigured Email Address

Unrestricted Email Address



Preconfigured Incoming Mail Server



Creating Mail Account Bundles

- Start with the .Mac bundle
- Use `uuidgen` to create unique IDs
- Edit as appropriate
- Provide a graphic
- /Library/Mail/AccountTypes/ca.bananasoftware.mailaccounts/
  - MailAccounts.plist
  - bananasoftware.ca.tiff

Summary

- Secure your mail
  - Disable plain text passwords
  - Enable SSL
  - Get S/MIME
- Filter your mail
  - RBLs
  - SpamAssassin
  - ClamAV
- Deploy a Mail account bundle

More Information

http://developer.apple.com/wwdc2005/

Documentation, Sample Code, and Other Resources

http://developer.apple.com/wwdc2005/

Related Sessions

Mac OS X Server Overview	Session 603 Tuesday 9:00AM
Moving to Tiger Server from Windows: A Primer	Session 612 Thursday 9:00AM
Upgrading to Tiger Server	Session 620 Wednesday 5:00PM
Managing Clients in the Enterprise	621 Wednesday 5:00PM
Enterprise Messaging Solutions	633 Friday 9:00AM

Q&A

Jason Anthony Guy
Manager, Developer Technical Support
jguy@apple.com

http://developer.apple.com/wwdc2005/

WWDC2005

Worldwide Developers Conference